Comments from Jim Basney - 2016-05-04

Subject:	Re: [Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 4 May 2016 12:41:24 +0000
From:	Basney, Jim <jbasney@illinois.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

On 4/21/16, 3:23 PM, David Walker wrote:

> *By the way, for those of you who may not have seen Monday's TIER release announcement, the MFA Interoperability Profile Working Group has asked that comments on its draft profiles and other documents be sent to assurance@incommon.org. Please take a look and weigh in on the conversation.*

I think this MFA profile is potentially very useful for enabling federated authentication to high-value scientific resources and instruments. I'm really glad to see this work progressing.
What process does the group envision for IdPs to be approved to assert http://id.incommon.org/assurance/mfa? Will it simply be a new checkbox on the As surance Addendum like http://id.incommon.org/assurance/bronze following the lightweight "Representation of Conformance" process?
Thanks,
Jim

Subject:	RE: [Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 4 May 2016 13:19:04 +0000
From:	Paul Caskey <pcaskey@internet2.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

I hope we don't need to require an addendum for MFA...

I think the intent was for self-assertion.

Subject:	RE: [Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 4 May 2016 13:48:10 +0000
From:	Cantor, Scott <cantor.2@osu.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

> I hope we don't need to require an addendum for MFA...
> > I think the intent was for self-assertion.

I won't speak for the WG, but while working on the material, I had been operating under the assumption this was not an assurance category at all but a self-asserted AuthnContextClassRef (in SAML terms), just like many others defined in SAML already. Thus the idea of a self-asserted category to go with a self-asserted AuthnContext seemed redundant (but that may prove not to be the case for other reasons). I didn't actually notice the naming convention in the URI included the word assurance, and tend to think that may be confusing as a result and worth reconsidering before this finalizes. Sometimes the obvious doesn't hit you when you're staring at it closely. -- Scott

---

Subject:	RE: [Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 4 May 2016 14:00:43 +0000
From:	Jokl, James A. (Jim) (jaj) <jaj@virginia.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

+1 I made it to many of the calls and always had the self-asserted picture in my mind as the basic perspective -- that this was about passwords no longer being adequate and what is the new baseline authentication. I still think of this stuff as "Standard Assurance" - good for whatever applications you used to just use and ID/Password for - but I get Scott's point too about the name. Note that this work took a nice low bar on the technical side - almost anything that you can call a second factor is acceptable -- and there is no discussion about identity proofing. All good for self-asserted, perhaps less so if people were thinking differently. Jim

---

Subject:	RE: [Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 4 May 2016 14:38:18 +0000
From:	Paul Caskey <pcaskey@internet2.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

+1 to all of that and yes, IMHO, we should not use the word 'assurance' to refer to this context.

Subject:	Re: [Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 4 May 2016 09:24:57 -0700
From:	David Walker <dwalker@internet2.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org

I'll take responsibility for putting the work "assurance" in the URI. I did it without much thought, and it certainly can be changed. In fact, the plan is to replace it with a URI in the REFEDS name space, anyway.

I agree with everyone that the MFA authentication context should be self-asserted. I think the real question is whether IdPs that support the MFA profile should also be given a (presumably self asserted) entity category in metadata. The current draft does not recommend an entity category, as the group didn't see use cases where it would help. We have since, however, heard of SPs that would like to tailor their discovery interfaces to exclude non-MFA-supporting IdPs, and there are situations where an entity category can save an SP from issuing a second authentication request when it prefers MFA, but will accept anything else.

Do others have use cases for an IdP entity category that it supports the MFA profile? It's certainly not too late to define one.

David

Subject:	RE: [Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 4 May 2016 16:35:02 +0000
From:	Paul Caskey <pcaskey@internet2.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

It was the discovery use case I had in mind...

Subject:	Re: [Assurance] comments on draft MFA Interop WG documents
Date:	Tue, 10 May 2016 04:00:01 +0000
From:	Herrington, Karen <kmherrin@vt.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

The MFA Interoperability Profile Working Group discussed this issue in its call last week, and we'd like some more input from all of you. Here's a summary of that discussion, followed by some questions for you.

Summary of Last Week's Discussion

There is a cost to creating entity categories. While it is relatively easy to define them (what the group has to do), there is also a cost to InCommon to modify its documentation and Federation Manager software. Further, assuming this becomes an international profile, all federations will bear that cost. Finally, this startup cost may be dwarfed by the ongoing effort on the part of IdP and SP operators, who must understand an increasing number of entity categories and react as appropriate.

So, we need to ensure that new entity categories bring value. These use cases have been identified for the use of an MFA entity category for IdPs:

1. Enable an SP to filter its discovery interface based on whether an IdP supports MFA.
2. Reduce the number of authentication requests an SP must issue to an IdP for certain types of error handling when MFA is desired, but other forms of authentication are acceptable.
3. Provide a formal mechanism for an institution to declare its compliance with the MFA profile (or perhaps a future stronger MFA profile).
4. Provide a workaround for SPs to avoid IdPs that do not behave as expected within the SAML spec. For example, they respond incorrectly to requests for specific authentication contexts (or they do not respond at all), or they crash.

The group had not previously discussed the discovery issue, but recognizes its importance; it's likely the most significant reason for defining an entity category. The group had earlier decided that the potential additional authentication requests didn't warrant an entity category, and that formal declaration of compliance was not necessary. The fourth issue of IdP behavior is broader than just the profiles defined by this group, and so out of scope, but it was recognized that definition of an MFA entity category would address that issue in this narrow instance.

Questions for You

1. If we define an MFA entity category, what should its criteria be? The group discussed the following:
    a. What does it mean for an IdP to “support MFA?” Is it the ability to issue assertions in compliance with the MFA profile for at least one member of its community? Something else?
    b. Should the ability to issue assertions in compliance with the Base Level profile also be included so that SPs that prefer MFA but will accept anything else can do that with a single authentication request? This would imply that the ability to assert Base Level be required of all members of the IdP’s community.
1. Would a formal institutional declaration of compliance with the MFA profile cause you to trust its MFA assertions more? Could that declaration be as simple as a box in the Federation Manager that would be checked by the site administrator, or should further documentation be required?

Thanks for your input,

Karen Herrington

Chair, MFA Interoperability Profile Working Group

Subject:	Re: [Assurance] comments on draft MFA Interop WG documents
Date:	Tue, 10 May 2016 13:41:50 +0000
From:	Basney, Jim <jbasney@illinois.edu>
Reply-To:	assurance@incommon.org
To:	InCommon Assurance <assurance@incommon.org>

```
Hi,

>What does it mean for an IdP to "support MFA?" Is it the ability to issue
>assertions in compliance with the MFA profile for at least one member of
>its community?

Yes.

In XSEDE we would conclude that researchers on that campus can use MFA for
federated authentication to XSEDE resources, so XSEDE doesn't need to
issue separate MFA tokens to those researchers. For more info on campus
researchers using XSEDE, see: https://www.xsede.org/campus-champions

>Should the ability to issue assertions in compliance with the Base Level
>profile also be included so that SPs that prefer MFA but will accept
>anything else can do that with a single authentication request?  This
>would imply that the ability to assert Base Level be required of all
>members of the IdP's community.

Yes.

I thought the InCommon Assurance program already defined a base LOA to
replace the POP. Any news on that?

>Would a formal institutional declaration of compliance with the MFA
>profile cause you to trust its MFA assertions more?

Yes.

>Could that declaration be as simple as a box in the Federation Manager
>that would be checked by the site administrator

Yes.

Sincerely,
Jim Basney
XSEDE's InCommon Site Administrator
>
```

Subject:	RE: [Assurance] comments on draft MFA Interop WG documents
Date:	Tue, 10 May 2016 14:46:02 +0000
From:	Cantor, Scott <cantor.2@osu.edu>

Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

```
> >Would a formal institutional declaration of compliance with the MFA
> >profile cause you to trust its MFA assertions more?
>
> Yes.

Can I ask why? What's the difference between self-asserting a category and self-asserting the same data in an
assertion?

-- Scott
```

Subject:	Re: [Assurance] comments on draft MFA Interop WG documents
Date:	Tue, 10 May 2016 16:12:28 +0000
From:	Basney, Jim <jbasney@illinois.edu>
Reply-To:	assurance@incommon.org
To:	InCommon Assurance <assurance@incommon.org>

```
>>>Would a formal institutional declaration of compliance with the MFA
>>>profile cause you to trust its MFA assertions more?
>>
>> Yes.
>
>Can I ask why? What's the difference between self-asserting a category
>and self-asserting the same data in an assertion?

I think my answer is the same for Base Level, MFA, Silver, or Bronze. Our
trust fabric is based on contractual agreements between InCommon LLC and
its participants, and that trust is operationalized via the federation
metadata. Knowing that an institutional representative made a declaration
to InCommon (either via an Assurance Addendum or via a checkbox on the
Federation Manager), subject to the Participation Agreement, gives me
greater trust in the organization's compliance with an InCommon standard
than I get from IdP-SP bidirectional communication alone.

-Jim
```

Subject:	RE: [Assurance] comments on draft MFA Interop WG documents
Date:	Tue, 10 May 2016 16:17:00 +0000
From:	Cantor, Scott <cantor.2@osu.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org <assurance@incommon.org>

> >Can I ask why? What's the difference between self-asserting a category
> >and self-asserting the same data in an assertion?
>
> I think my answer is the same for Base Level, MFA, Silver, or Bronze. Our
> trust fabric is based on contractual agreements between InCommon LLC and
> its participants, and that trust is operationalized via the federation
> metadata. Knowing that an institutional representative made a declaration
> to InCommon (either via an Assurance Addendum or via a checkbox on the
> Federation Manager), subject to the Participation Agreement, gives me
> greater trust in the organization's compliance with an InCommon standard
> than I get from IdP-SP bidirectional communication alone.

For the record, my counter-argument is that the the IdP is generally under the control of the same individual who would have to check that box, and who already vouched for the key with which the assertion is signed, and so it creates an extra step for that person. Multiplied across the federation, I think that's a real cost.

-- Scott